**POLÍTICA GESTIÓN DE COMUNICACIONES Y OPERACIONES**

**I.- DEFINICIONES ESTRATÉGICAS**

**a.- Objetivo general**

La empresa, a través de su [Comité de Riesgos y Seguridad de la Información], presenta en este documento la Política de Gestión de comunicaciones y operaciones.

En esta Política se busca establecer a la [Unidad TIC], como la Unidad encargada de la operación y de la administración de la plataforma tecnológica y soporte de los procesos automatizados.

**b.- Objetivos específicos**

Asegurar el cumplimiento mediante los requisitos normativos, estatutarios, reglamentarios y contractuales, que estén orientados la seguridad de la información en la empresa.

Analizar y establecer una adecuada gestión de comunicaciones y operaciones apropiados para la información de la empresa, brindando y asegurando la confidencialidad, integridad y disponibilidad que requiera cada sistema.

Apoyar e implementar el modelo de continuidad de negocio institucional (BCP por sus siglas en inglés) y de recuperación ante desastres (DRP por sus siglas en ingles) en cuanto a los elementos y plataforma tecnológica pertinentes. Las definiciones estratégicas necesarias para trabajar el BCP serán establecidas por el directorio o la gerencia general de la empresa.

Controlar y asegurar las instalaciones de procesamiento de información y datos de la empresa.

Establecer prácticas seguras de teletrabajo o trabajo a distancia mediante la utilización de tecnologías de la información y comunicaciones.

Securitizar, fortalecer las redes de la empresa administradas por la [Unidad TIC].

Apoyar y fortalecer las acciones tecnológicas y de ciberseguridad, ampliando el uso de tecnologías de información, mantención y control de las redes de datos y comunicaciones.

**c.- Alcance**

Esta política se aplica a todos los trabajadores y terceras partes que tengan o no una relación directa o indirecta de acceso a la información que pueda afectar los activos de información de la [Empresa XXX]. También se aplica a cualesquiera de sus relaciones con terceros que impliquen el acceso a sus datos, utilización de sus recursos o a la administración y control de sus sistemas de información.

Esta política rige independientemente del lugar en el trabajador presta sus servicios a la organización, total o parcialmente, e indistintamente de la modalidad de trabajo ya sea “presencial”, “a distancia”, “teletrabajo” u otra, en las condiciones que establezca la legislación vigente, los planteamientos de la Dirección del Trabajo o los Estados de Excepción Constitucional decretados por el Presidente de la República.

Esta política gobierna la seguridad de la información de todos los procesos estratégicos de la [Empresa XXX], establecidos en el documento institucional denominado Definiciones Estratégicas o equivalente, cubriendo a toda la organización independiente de su ubicación geográfica en el país (Chile Continental, Chile Insular o la Antártica Chilena).

**d.- Roles y Responsabilidades**

Las responsabilidades se encuentran definidas en la política de la organización de la seguridad de la información.

**e.- Vigencia y Actualización**

La Política se considera vigente desde la fecha de su aprobación por parte de la autoridad, documento que será revisado y actualizado cada dos años o cuando el Comité de Riesgos y Seguridad de la Información lo determine, o toda vez que se produzca un cambio significativo que modifique el nivel de riesgo presente de la [Empresa XXX].

La Política deberá ser revisada por el Comité de Seguridad de la Información. No obstante, aquello, la [Unidad responsable de Ciberseguridad] promoverá la revisión permanente de esta Política y generará las propuestas de actualización que sean necesarias, con el objetivo de apoyar el ciclo de mejora continua del SGSI.

Entre los cambios que hacen necesaria la revisión de las políticas, se debe destacar:

* Cambios en las leyes o reglamentos que afecten a la [Empresa XXX].
* Incorporación o modificaciones relevantes de procesos críticos de la [Empresa XXX].
* Cambios significativos al soporte tecnológico.
* Modificaciones en la estructura de la organización.
* Cambios significativos en los niveles de riesgo a que se expone la información.
* Cambios relevantes en las Definiciones Estratégicas.
* Ajustes necesarios producto de Estados de Excepción Constitucional.
* Ajustes necesarios para proteger las infraestructuras críticas.

Las revisiones que se efectúen a la Política de General de Seguridad de la Información deben considerar tanto la actualidad de ella, como su eficacia, eficiencia y cumplimiento.

**f.- Revisión del cumplimiento**

El Comité de Riesgos y Seguridad de la Información, anualmente, asignará la responsabilidad de ejecutar un proceso formal de revisión del cumplimiento a cargo de una o varias unidades organizacionales, pudiendo optar también por una revisión independiente interna o una externa ejecutada por una tercera parte.

Además, este Comité determinará la metodología y los alcances que estime necesarios para cumplir los objetivos estratégicos de revisión y cumplimiento de las políticas y su mejora continua.

**g.- Control de documentos**

Los documentos requeridos por el Sistema de Gestión de la Seguridad de la Información (SGSI) deben protegerse y controlarse. Con este objetivo, las acciones necesarias a implementar son:

* Revisar y actualizar los documentos cuando sea necesario y aprobarlos nuevamente.
* Registrar los cambios o actualizaciones de los documentos una vez que son aprobados por el Comité de Riesgos y Seguridad, incorporando Tabla en Capitulo final en cada documento.
* Se deberá controlar el uso no intencionado de documentos obsoletos.
* En caso de mantenerse los documentos por cualquier propósito, éstos deberán tener una adecuada identificación a efecto de diferenciarse de los vigentes.

Las versiones pertinentes de los documentos aplicables se encontrarán disponibles para quienes lo necesiten y serán almacenados y transferidos de acuerdo con los procedimientos aplicables a su clasificación.

**h.- Difusión**

El mecanismo de difusión de la Política será a través de la Intranet, circulares informativas, correos electrónicos masivos o cualquier otro medio que el Comité de Riesgos y Seguridad de la Información estime pertinente, procurando apoyar la sensibilización con infografías que faciliten la comprensión de esta por todos los usuarios en general.

**II.- GESTIÓN DE COMUNICACIONES Y OPERACIONES**

**a.- Procedimientos operacionales y responsabilidades**

A continuación, se establecen responsabilidades con respecto a la gestión y operación de las tecnologías de la información y comunicaciones: la [Unidad TIC] evaluará los contratos y acuerdos con terceros para garantizar la incorporación de aspectos relativos a las tecnologías de información y comunicaciones, así como también la seguridad de la información involucrada en la gestión de productos y servicios prestados.

**Documentación de los procedimientos tecnológicos**

Los procedimientos tecnológicos identificados en esta política específica de comunicaciones y operaciones y sus cambios serán gestionados por el Jefe de [Operaciones de la Unidad TIC], los cuales se refieren a las siguientes actividades y funciones:

* Control de cambios sobre la plataforma tecnológica.
* Aprobación, implementación de nuevos productos y servicios tecnológicos.
* Instalación de nuevas versiones/actualizaciones.
* Implementación de la mitigación de incidentes y vulnerabilidades.
* Uso correcto del correo electrónico, internet, usuario empresarial, certificado digital.
* Administración de identidades.
* Control de acceso.
* Protección contra software malicioso.
* Detección y prevención de intrusiones.
* Protección de usuarios con altos privilegios.
* Uso de dispositivos de almacenamiento extraíbles.
* Elaboración y recuperación de copias de respaldo.
* Borrado seguro de información.
* Eliminación de dispositivos de almacenamiento.
* Gestión de logs.
* Reinicio del sistema y procedimientos de recuperación ante fallas.
* Instalación y mantenimiento de equipos de procesamiento y comunicaciones.
* Instalación y mantenimiento de plataformas computacional.
* Monitoreo del procesamiento y comunicaciones.
* Administración de claves de equipos de comunicación.
* Apoyar la gestión y procedimientos de Incidentes de ciberseguridad.
* Apoyar la gestión y procedimientos del Equipo de Respuesta ante Incidentes de Ciberseguridad con funcionamiento 7x24.
* Documentar y realizar procedimientos para el plan de continuidad de negocio institucional (BCP por sus siglas en inglés).
* Documentar y realizar procedimientos para el plan de recuperación ante desastres institucional (DRP por sus siglas en inglés).
* Desarrollar operaciones y procedimientos que sean necesarios para el funcionamiento resiliente, correcto y seguro de la plataforma tecnológica institucional en modalidad 7x24.

**Control de cambio en las operaciones**

Todo cambio deberá ser evaluado previamente, tanto en los aspectos técnicos de funcionalidad como de seguridad acorde con el procedimiento para el control de cambios sobre la plataforma tecnológica.

Los registros de los cambios deberán documentarse y contemplarán los siguientes puntos que dependerán de si se trata de proceso planificado o de emergencia; en este último caso no se realizan las actividades de planificación:

* Identificación de la modificación y registro de cambios.
* Análisis de riesgo del cambio.
* Aprobación formal del cambio.
* Planificación del proceso de cambio.
* Prueba del nuevo escenario.
* Comunicación del cambio a todas las partes interesadas.
* Identificación de los responsables del cambio.
* Procedimiento para cancelación del cambio en caso de fallo.
* Verificación del cambio realizado.
* Documentar incidente, en caso de emergencia.

**Distribución de funciones**

Se requerirá la provisión de ambientes de trabajo separados para desarrollo, pruebas y producción para las instancias de [Desarrollo de Software] y [Explotación de Sistemas], ambas llevadas adelante por la [Unidad TIC].

De no ser posible la segregación de funciones, por razones presupuestarias, de personal u otro tipo, se implementarán controles adicionales tales como:

* Todos los equipos de procesamiento y comunicaciones deberán tener activadas las auditorías que generan los archivos de logs y enviarlos a un repositorio central recolector de logs (*syslog o rsyslog* por el nombre de una de las implementaciones posibles), como proceso básico mínimo obligatorio. En una fase avanzada esta técnica puede ser complementada o integrada a un sistema SIEM.
* Complementariamente se implementarán sistemas de detección de intrusos, separación de redes mediante equipamiento tecnológico adecuado, y se procurará la integración de tecnologías de análisis y correlación de eventos (SIEM por sus siglas en inglés) y tecnologías de automatización de tareas (SOAR por sus siglas en inglés).
* La [Unidad TIC] supervisará y monitoreará las transacciones realizadas sobre los sistemas y equipos de procesamiento y comunicaciones.

**Separación de ambientes de desarrollo, pruebas y paso a producción**

Los ambientes de desarrollo, pruebas y su paso a producción, estarán separados en sus aspectos operacionales. La transferencia de software del ambiente de pruebas al ambiente de producción será debidamente documentada por sus responsables. Si estas funciones están externalizadas deberá procurarse que el proveedor cumpla estos estándares mínimos.

Los pasos a producción deberán cumplir con las siguientes definiciones de trabajo:

* Ejecutar el software de desarrollo y producción en diferentes ambientes.
* Las actividades de desarrollo y pruebas deberán realizarse en ambientes separados.
* Los datos de producción no deberán usarse en ambientes de desarrollo o pruebas.
* El uso de software de desarrollo deberá estar alineado con los ambientes de producción.
* Limitar el acceso del personal de desarrollo al ambiente de producción, a menos que sea estrictamente necesario, razones que deberán quedar registradas y documentadas, incluyendo la individualización del personal involucrado.

**b.- Gestión de la prestación de servicios por terceras partes**

La empresa necesita contratar servicios especializados externos que den soporte a parte de su actividad. En estos casos de nada sirve asegurar los sistemas si no se exige la misma seguridad a los proveedores externos para que puedan gestionar parte la información de la empresa (sobre todo si es información confidencial o sensible en los términos de la Ley N° 19.628). Entre estos proveedores podemos destacar los siguientes grupos:

* Proveedores de servicios tecnológicos. Aquellos que ofrecen servicios como alojamiento web, emisión de certificados, servicio *gateways* de pago, servicios de almacenamiento en la nube, servicios de soporte informático (tanto presencial como remoto), etc.
* Proveedores de servicios no tecnológicos, pero que acceden a datos corporativos. Tales como proveedores de servicios financieros, viajes, transporte, publicidad y marketing, etc.
* Suministradores de productos tecnológicos. Incluyen todos aquellos dónde se adquieren los dispositivos, los componentes de hardware y las aplicaciones informáticas.

La conectividad y complejidad de los sistemas de información actuales hacen indispensable mantener el control sobre la seguridad de la informaciónde la empresa, aun cuando esta esté siendo gestionada por terceros.

La tercerización de la plataforma tecnológica estará supeditada a los controles establecidos en el contrato, contemplando las especificaciones descritas en la Política específica “Organización de la seguridad de la información”.

Asimismo, se contemplará las siguientes premisas, antes de tercerizar los servicios de procesamiento:

* Identificar los riesgos de aquellos servicios y/o infraestructura que se requiera encargar a terceros.
* Contar con la aprobación de los dueños de los activos de información, antes de efectuar la tercerización.
* Identificar las aplicaciones que manejan información Confidencial, Interna y Pública de la empresa, con el fin de contemplar medidas de seguridad más fuertes antes de su tercerización.
* Monitorear permanentemente el servicio externalizado con el fin de evaluar el cumplimiento de los acuerdos de niveles de servicio y de no divulgación (NDA por sus siglas en inglés).
* Monitorear permanentemente el servicio externalizado con el fin de evaluar el cumplimiento de los acuerdos confidencialidad.
* Definir las funciones y procedimientos de comunicación y manejo de incidentes relativos a la seguridad.

A continuación, se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo a relación con proveedores.

Los controles podrán tener el siguiente alcance:

* Requisitos de seguridad en productos y servicios
	+ Establecer los requisitos de seguridad mínimos que deben cumplir los productos que se adquieren y los servicios que se contratan.
* Definir cláusulas contractuales en materia de seguridad de la información
	+ Ser riguroso en la elaboración y aceptación de las cláusulas contractuales en materia de ciberseguridad.
* Definir las responsabilidades concretas por ambas partes
	+ Delimitar las responsabilidades en materia de ciberseguridad para cada una de las partes involucradas.
* Definir los SLA (Acuerdos de Nivel de Servicio)
	+ Definir en detalle los SLA a los que someten los servicios contratados.
* Controles de seguridad obligatorios
	+ Determinar que controles de seguridad son de cumplimiento obligatorio en las relaciones con los proveedores de servicios tecnológicos.
* Formar parte de los foros y organizaciones de usuarios de los productos/servicios software utilizados
	+ Participar en las organizaciones de usuarios de los productos y servicios software que se adquieren. Controlar la reputación de los proveedores.
* Certificación de los servicios contratados
	+ Exigir a los proveedores certificaciones que garanticen la calidad en materia de seguridad de ciertos servicios contratados de especial criticidad.
* Auditoría y control de los servicios contratados
	+ Supervisar que los productos y servicios contratados responden a lo acordado en materia de ciberseguridad.
* Finalización de la relación contractual
	+ Garantizar la seguridad de la información tras la finalización de un servicio o contrato. Generalmente controlado por el establecimiento de acuerdos de no divulgación o NDA.

**c.- Planificación y aceptación de sistemas**

**Planificación de la Capacidad**

La [Unidad TIC], realizará un análisis estadístico anualmente para generar líneas base que le permitan proyectar necesidades de crecimiento en procesamiento, almacenamiento y transmisión de la información, con el fin de evitar situaciones que puedan constituirse en una amenaza a la continuidad de los servicios prestados. Asimismo, la [Unidad TIC] analizará la obsolescencia tecnológica de las plataformas que puedan incidir en los niveles de disponibilidad y seguridad.

**Aceptación del sistema**

La [Unidad TIC], realizará pruebas a los sistemas antes de su salida a producción teniendo en cuenta lo siguiente:

* Analizará cómo afecta el nuevo sistema o sus actualizaciones la capacidad de procesamiento y almacenamiento de los sistemas actuales.
* Garantizará la recuperación ante errores.
* Contará con mecanismos de restauración del sistema a su estado inicial antes del cambio.
* Validará que el nuevo sistema implementado no afecte a los sistemas actuales de producción.
* Someterá a pruebas de funcionalidad y seguridad a todo sistema antes de salir a producción.
* Los usuarios de los nuevos sistemas deberán ser capacitados en su uso, en caso de ser necesario.
* Interoperabilidad con plataforma y sistemas existentes en la Organización con entidades externas de gobierno.

**Análisis de Riesgo**

Toda puesta en producción de los Sistemas, intercambio de datos y otros procedimientos, deberán pasar por un análisis de riesgos, un análisis de vulnerabilidades, un test de penetración, un ethical hacking y un análisis de cumplimiento normativo que permitan establecer los posibles puntos de falla que no satisfagan las condiciones de confidencialidad, integridad y disponibilidad; debilidades que en caso de presentarse deberán ser corregidos mediante la coordinación de la [Unidad TIC] o los proveedores del servicio según corresponda. Este proceso será iterativo hasta que se satisfagan los niveles de riesgo residual exigidos por la empresa y verificados por la [Unidad TIC], la que deberá velar por el adecuado equilibrio de esfuerzo tecnológico, económico y coherencia con las directrices del negocio; siempre teniendo en cuenta nos niveles de clasificación de la información tratada y actuando en consecuencia con mayor celo para aquellos sistemas que involucren información Confidencial o Interna o de la infraestructura crítica de la empresa o de cualquier entidad ya sea pública o privada que esté en su poder.

**Protección Contra Código Malicioso**

La aparición constante de nuevos virus y otros tipos de malware o código malicioso es una de las principales amenazas a las que se enfrentan hoy en día los sistemas de las empresas.

Las vías de contagio por malware son numerosas, destacando entre otras:

* las descargas de ficheros de todo tipo, adjuntos en correos o desde páginas web;
* la navegación por webs de dudosa fiabilidad;
* y la utilización de dispositivos ajenos, por ejemplo, pendrives.

El enorme daño que pueden causar a la empresa hace obligatorio el establecimiento de una política de control de malware. De este modo se podrá prevenir, detectar, controlar y eliminar la ejecución de cualquier software malicioso en los sistemas.

La [Unidad TIC], implementará controles para prevenir y detectar código malicioso, lo cual se basa en software, concientización de usuarios y gestión del cambio. Los controles contemplan las siguientes directrices:

* Impedir el uso de software no autorizado.
* Impedir el compartir carpetas en los computadores y/o dispositivos personales.
* Implementar acciones y procedimientos para evitar los riesgos relacionados con la obtención de archivos y software desde o a través de redes externas, o por cualquier otro medio, señalando las medidas de protección a tomar en procedimientos de soporte a usuarios.
* Instalar y actualizar software de detección y reparación de virus, IPS de host, anti- spyware examinado computadores y medios informáticos, como medida preventiva y rutinaria.
* Mantener los sistemas con las últimas actualizaciones de seguridad disponibles, previa realización de pruebas en un ambiente dispuesto para tal fin.
* Chequear periódicamente el contenido de software y datos de los equipos de procesamiento, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas.
* Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos de origen incierto, o en archivos recibidos a través de redes no confiables.
* Informar al personal acerca del problema de los falsos virus y de cómo proceder frente a los mismos.

Los aspectos estratégicos para el éxito de esta tarea son:

Determinar qué tipo de soluciones serán las más convenientes para la empresa. Dependiendo del tamaño, del nivel de seguridad necesario y de la complejidad de las configuraciones para la protección de los activos de información, se podrá determinar distintos tipos de soluciones:

* herramientas para el puesto de trabajo, el portátil o los dispositivos móviles,
* soluciones globales corporativas entre ellas:
	+ UTM o gestión unificada de amenazas;
	+ servicios gestionados que nos pueden facilitar loss proveedores de servicios de internet (ISP) u otros proveedores desde un centro de operaciones de seguridad o SOC;
	+ soluciones de seguridad ofrecidas como servicios en la nube que monitorizan los equipos de forma remota.

Para el tipo de solución elegida, se seleccionará la más apropiada de entre las disponibles en el mercado buscando la compatibilidad con las infraestructuras y la versatilidad (antimalware, antiphishing, antispam, análisis de web y correo entre otros) de la herramienta.

Configurar las herramientas de detección de malware. Para un uso eficiente de las herramientas de control de malware se deberá realizar una correcta configuración de todas sus funcionalidades. La configuración deberá permitirnos, entre otros, establecer los siguientes controles:

* realizar análisis automáticos y periódicos para detectar malware;
* realizar comprobaciones automáticas de los ficheros adjuntos al correo y de las descargas web, ya que pueden contener código malicioso ejecutable;
* bloquear el acceso a ciertas aplicaciones o sitios web basándonos en una política de listas negras;
* permitir el acceso a ciertas aplicaciones o sitios web basándonos en una política de listas blancas;
* permitir el análisis de páginas web para detectar posibles amenazas incluidas en las mismas.

Actualizar las herramientas de detección de malware. Se deberá determinar la periodicidad con la que las herramientas de detección de malware son actualizadas. Actualmente se crean miles de virus al día, por lo que las actualizaciones de la base de datos de firmas de virus deberían ser automáticas y tener una periodicidad como mínimo diaria. Por otro lado, y como cualquier otra aplicación crítica, tendremos que actualizar convenientemente el propio software antivirus y el sistema operativo del servidor que permite su funcionamiento.

Establecer el procedimiento de respuesta ante la infección por ejecución de malware. En primer lugar, se deberá determinar qué sucesos serán considerados como incidencias por ejecución de malware, analizando:

* el impacto del ataque;
* los activos que puedan estar comprometidos;
* la forma de recuperar los activos impactados;
* los canales adecuados de aviso y notificación.

Después se establecerán las responsabilidades y la operativa a seguir en cada caso:

* desinfección de archivos y documentos;
* eliminación de archivos y documentos;
* aviso a soporte técnico del fabricante;
* reinstalación de software afectado;
* desconexión y asilamiento del equipo afectado;
* y el registro formal del incidente.

Política general de buenas prácticas para el control de malware. Con el fin de reforzar las medidas establecidas para el control del malware es conveniente tener concienciado al personal en los siguientes aspectos:

* Se deben considerar todos los contenidos y las descargas como potencialmente inseguros hasta que no sean convenientemente analizados por una herramienta de detección de malware.
* Deben prohibirse las siguientes acciones:
	+ Ejecutar archivos descargados de servidores externos, de soportes móviles no controlados o adjuntos a correos, sin haber sido previamente analizados.
	+ Configurar el programa cliente de correo electrónico para la ejecución automática de contenido recibido por correo.
	+ Alterar la configuración de seguridad establecida para los sistemas y equipos de tratamiento de información.
* Debe utilizarse únicamente el software permitido la empresa. Este además debe estar convenientemente actualizado y licenciado.
* Para evitar la recepción de spam se deben seguir las directrices incluidas en la política de correo electrónico.

**d.- Respaldo**

La [Unidad TIC], junto con los propietarios de los activos de información, determinará los requerimientos de respaldo, según su nivel de criticidad, nivel de riesgo, asegurando la confidencialidad, integridad y disponibilidad de la información.

Los respaldos son gestionados y administrados por la [Unidad TIC], cuidando el equilibrio de recursos tecnológicos y económicos disponibles, así como la clasificación de confidencialidad, integridad y disponibilidad de la información involucrada.

**Metodología de Respaldo**

El procedimiento de respaldo de la información incluye actividades de prueba de recuperación de la información. Las instalaciones de resguardo garantizarán las condiciones de seguridad ambientales necesarias para la conservación de los respaldos. El procedimiento de respaldo de la información contempla las siguientes directrices:

* Disponer un esquema de rótulo de las copias de respaldo, para permitir su fácil identificación.
* Destruir las copias de respaldo, cuando expire la vida útil de los medios de almacenamiento, de acuerdo con el procedimiento de destrucción o reutilización segura de equipos.
* Almacenar las copias de respaldo en un lugar fuera de las instalaciones del sitio de origen de la información, manteniendo un registro exacto y completo de cada una de ellas, así como de los procedimientos de restauración aplicados.
* Almacenar las copias de respaldo en condiciones de seguridad y ambientales adecuadas, consistentes a las aplicadas al sitio principal.
* Probar periódicamente la restauración de los medios de respaldo.
* La información de LOG’s de auditoría, de seguridad y de los sistemas se mantendrá con una historia de por lo menos 1 año.

**Consideraciones especiales para uso de almacenamiento en la nube**

Algunas razones para almacenar información de la empresa en la nube son:

* acceder a la información desde cualquier dispositivo y lugar;
* ahorro de recursos y ahorro económico;
* proporciona directorios compartidos con distintos permisos de acceso;
* y permite el trabajo colaborativo sobre un documento.

Antes de proceder a su implantación en la empresa deben valorarse los aspectos negativos como la dependencia de terceros o la necesidad de conexión a internet para tener acceso a la información.

Para que el personal haga un buen uso de los recursos de almacenamiento, la empresa dispone de una Política de clasificación de la información, donde se indica qué tipo de información puede subirse a la nube.

Junto a esta clasificación se elabora una normativa interna para el tratamiento de la información crítica y sensible, que indica cuándo debe ir cifrada y otras medidas de seguridad que le aplican como respaldos o borrado seguro de la información.

Los puntos clave a tener en consideración sobre el uso de almacenamiento en la nube:

Uso de servicios de almacenamiento en la nube públicas. La empresa debe decidir si está permitido el uso de servicios de almacenamiento nube pública. El personal no podrá utilizar este tipo de repositorios si así lo contempla la normativa de la empresa.

Lista de servicios de almacenamiento en la nube permitidos. La empresa dispone de una lista de los servicios de almacenamiento en la nube permitidos y prohibidos. De esta forma se evita el uso de servicios de almacenamiento que son considerados como no seguros.

Proceso de borrado de la información. Se aplicará una Política de borrado de la información que también se debe aplicar cuando se elimina información almacenada en la información en la nube.

Tipo de información almacenada. El personal debe conocer qué tipo de información puede almacenarse en la nube (y cual no) y en qué casos tendrá que almacenarse cifrada. La política de clasificación de la información incluye este dato.

Copias de seguridad en la nube. El personal tendrá presente las ventajas e inconvenientes de realizar copias de seguridad en la nube antes de realizarlas.

* Ventajas:
	+ Disponer de más espacio para realizar la copia de seguridad a medida que lo necesitemos.
	+ La mayoría de los servicios en la nube realiza copias de seguridad como garantía de disponibilidad.
	+ Disponer de una copia fuera de las dependencias de la empresa. En caso de que se produjera un incidente, nuestra información no se vería afectada y podríamos recuperarla.
* Inconvenientes:
	+ Depender de terceros que tendrán sus riesgos propios que pueden quedar fuera de nuestro control.

Contratación de servicios de almacenamiento en la nube. Al contratar un servicio de almacenamiento en la nube, la empresa se asegurará que cumple con los criterios de seguridad específicos que precisa la información que se va a almacenar en la nube (garantía de confidencialidad, disponibilidad de la información, copias de seguridad, información de auditoría, etc.), así como con las necesidades legales si se trataran de datos personales.

Política de seguridad del proveedor. Antes de contratar servicios en la nube que traten información de la empresa, Confidencial e Interna o de datos personales, se debe leer y comprender la política de seguridad del proveedor de servicios para asegurar que cumple todas las necesidades de la empresa y legislación vigente sobre la materia.

**e.- Gestión de la seguridad en la red**

**Controles de las redes**

La [Unidad TIC] definirá los controles de seguridad de la red de comunicaciones e información en la empresa. Estos controles contemplarán salvaguardas especiales para:

* Los equipos activos en las redes de área local.
* Mantener la disponibilidad de los servicios de red e infraestructura tecnológica conectados.
* La transmisión de información a través de redes públicas.
* El acceso a la red institucional, desde otras redes.
* El intercambio de información interinstitucional con el sector público y privado.
* Garantizar la trazabilidad de las conexiones a la red institucional.
* Supervisión del cumplimiento de los controles implementados.
* Criptografía a utilizar para la seguridad del intercambio de comunicaciones e información.

**Seguridad de los servicios de red**

Los acuerdos de niveles de servicio (SLA) y de confidencialidad (NDA) contemplarán, características de seguridad, requisitos de gestión de los servicios de red y valores agregados en dispositivos de seguridad. Asimismo, estarán documentados los procedimientos para:

* Chequeo del tráfico de la red.
* Nivel de utilización de los servicios respecto de lo contratado
* Parámetros técnicos para los enlaces de comunicaciones como latencia, tiempo de respuesta, jitter, tasa de errores en las interfaces, tasa de pérdidas de paquetes
* Uso de las instancias de redundancia ya sea de los equipamientos como de los enlaces
* Sistema de monitoreo por parte del proveedor que se contrastarán con los sistemas de monitoreo internos
* Monitoreo de los puertos en la red.
* Auditoría, trazabilidad y respaldo de archivos de logs.
* Correlación de eventos
* IDS/IPS internos
* Firewall Internos para separación de redes
* Informes de cumplimiento tanto del proveedor como de los monitoreos internos

**f.- Servicio de Soporte Técnico.**

La [Unidad TIC], se encargará de velar por el uso y funcionamiento de la plataforma tecnológica de la institución y asegurar la asistencia técnica a los funcionarios.

Actividades y funciones:

* Llevar un inventario de la infraestructura tecnológica administrada por la División.
* Determinar la vida útil de los equipos informáticos.
* Apoyo en las especificaciones técnicas, en las solicitudes de compra.
* Realizar el mantenimiento técnico preventivo de todos los equipos informáticos a su cargo.
* Encargado de configurar e instalar los equipos computacionales y todo software requerido y debidamente licenciado para su funcionamiento.
* Tener un control del licenciamiento de software adquirido.
* Llevar registro del movimiento de los equipos tecnológicos asignados, teniendo la obligación de informarlo al área responsable del inventario institucional.
* Administración y gestión de cuentas de usuarios de la red institucional de acuerdo con el perfil de usuarios que se indican en Política de uso de equipamiento de la empresa.

El soporte técnico a los usuarios se provee a través de plataforma de mesa de ayuda para gestión de solicitudes de soporte técnico, el cual acepta múltiples entradas: correo electrónico, llamadas telefónicas y presenciales.

Sólo se entregará soporte técnico a equipos y software de la empresa.

**g.- Intercambio de información**

El intercambio de información con terceras partes se formalizará a través de Convenio aprobado por la [gerencia general], en el que se establezcan cláusulas de responsabilidad, deberes y derechos.

En todos los casos, estos acuerdos deben velar por el cumplimiento de las regulaciones legales, propiedad intelectual y protección de datos personales. Asimismo, se deberán especificar las consideraciones de seguridad y reserva de la información y las responsabilidades por el mal uso o divulgación de esta (NDA).

El intercambio de información contemplará las siguientes directrices:

* Uso de webservices, para la publicación y uso de información electrónica.
* Uso de canales cifrados.
* Respeto por los derechos de autor del software intercambiado, por tratarse de un bien de la entidad.
* Términos y condiciones de la licencia bajo la cual se suministra el software.
* Uso de un sistema convenido para el rotulado de información clasificada, garantizando que el significado de los rótulos sea inmediatamente comprendido por el receptor de la información.
* Mantener informado al dueño de los datos, acerca del proceso del intercambio de éstos con otras entidades.
* Deberá aplicar, en lo posible, controles de ciberseguridad como los señalados en el estándar ISO 27.010, cuando se trate de información clasificada como Confidencial, de infraestructuras críticas o de terceras partes.

**Medios físicos en tránsito**

El transporte de información en medios físicos (digital o impresa) deberá contemplar mecanismos de seguridad. Los controles establecidos para el transporte de información contemplarán:

* Uso de servicios de mensajería, a través de contratos formales en caso de servicio externo, donde se establezcan los acuerdos de niveles de servicio que contemplen los mecanismos de seguridad y oportunidad que deberá ser proporcionado por el contratista.
* Deberá aplicar, en lo posible, controles de ciberseguridad como los señalados en el estándar ISO 27.010, cuando se trate de información clasificada como Confidencial.

Los acuerdos de niveles de servicio con entidades prestadoras deberán contemplar como mínimo:

El uso de recipientes cerrados.

* La entrega certificada del envío.
* Embalaje con sellos de seguridad o a prueba de apertura no autorizada.
* La entrega física de información realizada por funcionarios de la institución deberá cumplir con las mismas características, estipuladas en el punto anterior.

**Medios Electrónicos**

La información que se transfiera por vía de mensajería electrónica será efectuada a través de la plataforma de correo electrónico institucional, regulada por la “Política de Uso de Correo Electrónico Institucional”.

En caso de utilización de otros medios electrónicos (ssh, sftp, vpn y otros) la transferencia deberá ser efectuada utilizando canales seguros, precisando su origen y destino, donde la criptografía empleada se sustente en algoritmos robustos y fuertes.

Se deberá aplicar, en lo posible, controles de ciberseguridad como los señalados en el estándar ISO 27.010, cuando se trate de información clasificada Confidencial.

**Sistemas de acceso público**

Toda la información pública disponible en sistemas y sitios web institucionales, será resguardada de posibles modificaciones que afecten la imagen institucional.

Se establecerá un procedimiento formal para la publicación de información en los sitios web, antes que ésta sea puesta a disposición de la ciudadanía en internet. El contenido que se pública es de responsabilidad de los encargados autorizados de las publicaciones.

**Monitoreo**

Con el fin de evitar el mal uso de la plataforma tecnológica institucional y evidenciar actividades sospechosas o posibles fallas, la [Unidad TIC], realizará labores de monitoreo sobre las transacciones realizadas en los sistemas de información.

**Registro de auditorias**

Los sistemas de información, así como los servidores, dispositivos de red y demás servicios tecnológicos, deberán guardar registros de auditoría y logs, los cuales contemplarán, siempre y cuando sea posible:

* Id del usuario.
* Fecha y hora de la transacción.
* Dirección IP y nombre del dispositivo desde el cual se realizó la transacción.
* Tipo de transacción.
* Intentos fallidos de conexión.
* Cambios en la configuración del sistema.
* Cambio o revocación de privilegios.
* Alarmas originadas por los sistemas de monitoreo.
* Desactivación de los mecanismos de protección.
* acceso, creación, borrado y actualización de información confidencial;
* inicio y fin de conexión en la red corporativa;
* inicio y fin de ejecución de aplicaciones y sistemas;
* inicio y fin de sesión de usuario en aplicaciones y sistemas; intentos de inicio de sesión fallidos;
* cambios en las configuraciones de los sistemas y aplicativos más importantes;
* modificaciones en los permisos de acceso;
* funcionamiento o finalización anómalos de aplicativos;
* aproximación a los límites de uso de ciertos recursos físicos:
	+ capacidad de disco;
	+ memoria;
	+ ancho de banda de red;
	+ uso de CPU;
* indicios de actividad sospechosa detectada por antivirus, Sistemas de Detección de Intrusos (IDS), etc.;
* transacciones relevantes dentro de los aplicativos.

Teniendo en cuenta las múltiples fuentes de datos de registros de logs y auditorías, éstos se almacenarán en repositorio digital concentrador de eventos (un servidor de *syslog* como implementación mínima), cuya capacidad estará sujeta a la disponibilidad de recursos, procurando mantener una historia de al menos 1 año de eventos y LOGS.

Para cumplir con el adecuado aseguramiento de estos importantes datos se deben chequear los siguientes temas:

* Qué actividad debe ser registrada
* Información relevante incluida en el registro
* Formato de la información registrada
* Elección del mecanismo de registro
* Protección y almacenamiento
* Sincronización del reloj
* Sistemas de monitorización y alerta

Información relevante incluida en el registro. Los más habituales son:

* identificador del usuario que realiza la acción;
* identificación del elemento sobre el que se realiza la acción (archivos, documentos, bases de datos, equipos, etc.);
* identificación de dispositivos, ya sea a través de sus direcciones IP, direcciones MAC, etc.;
* identificación de protocolos;
* fecha y hora de ocurrencia del evento;
* tipología del evento.

**Protección de los registros de auditoría**

El acceso a los registros de auditoría deberá ser salvaguardado de acceso o modificaciones, que alteren su integridad, para lo cual su acceso es restringido al encargado de seguridad y de sistemas.

Estos registros deberán poseer copias de respaldo, en la medida que se disponga de recursos, procurando mantener una historia de al menos 1 año de eventos y LOGS.

**Sincronización de relojes**

Para garantizar la exactitud de los registros de auditoría, la [Unidad TIC], dispondrá de un servicio de protocolo de tiempo de red NTP que estará sincronizado a su vez con la hora oficial de Chile Continental; servicio que en la actualidad provee el Servicio Hidrográfico y Oceanográfico de la Armada de Chile (SHOA).